

Brad Judy

brad.judy@gmail.com

INFORMATION SECURITY PROFESSIONAL

Certified Information Systems Security Professional with experience in information technology risk assessment, regulatory compliance, vulnerability assessment, incident response and information security awareness. Active in the higher education technology community (REN-ISAC, Educause, Windows in Higher Education). **Skills include:**

- Information technology risk assessment
- Regulatory compliance (HIPAA, PCI-DSS, FERPA)
- Technology selection, deployment, management and support
- Technical staff management
- Service architecture
- Business analysis
- Presentations and documentation

EXPERIENCE

Emory University and Healthcare, Atlanta, GA

5/2009 – Present

Senior Information Security Specialist

Serve as technical lead on information security related projects, provide security guidance for other technology projects, co-author institutional security policies, provide security consulting services for departments across the institution and serve as primary author and presenter of information security awareness content..

Key projects:

- Institution-wide PCI-DSS compliance initiative technical lead – train both business and technical groups on PCI-DSS, lead the process to evaluate and select Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV), analyze PCI requirements and determine necessary IT tasks and projects
- Security information and event management (SIEM) project technical lead – evaluated, selected and deployed a Q1 Qradar security event management system processing 400 million events per day, including creating custom parsers, rules and reports.
- Whole disk encryption project technical lead – deployed infrastructure for PGP whole disk encryption, developed documentation and provide escalated PGP support to departmental IT staff over the course of deployments to hundreds of laptops.

University of Colorado at Boulder, Boulder, CO

1/2000 – 5/2009

Messaging analyst (12/2008 - 5/2009)

Provided remote consulting role for a project to both upgrade the existing Exchange 2003 infrastructure to Exchange 2007 and expand its use from select departments to all employees on the UC-Boulder campus.

Key projects:

- Exchange 2007 upgrade and service expansion project planning and design

Senior IT Security Analyst (6/2006 - 6/2008)

Served as technical lead on information security related projects, managed IT personnel, provided security guidance for other technology projects, provided security consulting services for departments across the institution co-author institutional security policies, and served as primary incident responder for major incidents.

Key projects:

- Lead for IT risk assessment for Boulder Campus – developed campus IT risk assessment process (based on NIST 800, CERT OCTAVE, etc) and performed IT risk assessments of key departments resulting in department-created risk mitigation timelines

- Private data security – lead role for campus PCI-DSS security (liaison to card handling departments, treasury department and external scanning vendor), developed private data identification process (selected tools and developed a process for campus-wide private data identification and reporting)

IT Architect (6/2003 - 7/2006)

Provided service architecture for enterprise IT projects including requirements gathering, use-case analysis, and high-level design. Acted as project manager for projects, including vendor relationship management.

Key projects:

- WebCT 4 to WebCT CE6 upgrade architect and project manager – deployed new hardware, application and support elements in time for faculty to learn the new version before the fall semester
- Spam filtering replacement architect and project manager – selected and deployed Barracuda Networks appliances resulting in significantly decreased spam delivery and improved tagging of potential spam
- Student web file system architect and project manager – deployed a new service based on the Xythos WFS product, providing online file storage to 30,000 students

Active Directory Administrator (1/2000 - 6/2003)

Part of a two-person team that deployed and managed the campus-wide Active Directory infrastructure.

Key projects:

- Design, implementation, administration and support of campus-wide central Active Directory service leveraging MIT Kerberos authentication and existing Unix-based DNS/DHCP infrastructures. Grew the service to include 50,000+ user accounts and 3,000+ computer objects.
- Upgraded the root domain to Windows Server 2003 and coordinated the independently operated child domain upgrades to a 2003 forest functional level
- Deployed an Exchange 2003 messaging service from the ground up for campus executives, designed to expand to additional campus users

EDUCATION & CERTIFICATIONS

University of Colorado at Boulder, Boulder, CO

5/2000

- Bachelor of Arts - Sociology

Certifications

- Certified Information Systems Security Professional (CISSP)
- Tripwire Enterprise certified professional
- PGP Certified Technician

PROFESSIONAL ACTIVITIES

Research and Education Network – Information Sharing and Analysis Center (REN-ISAC)

9/2006 – Present

- Membership committee vice-chair – Participate in evaluating applications for membership and addressing violations of information sharing guidelines.
- Founding member, Microsoft Analysis Team – Provided analysis and guidance on security issues related to Microsoft technologies and products to higher education community via REN-ISAC

Windows in Higher Education

8/2000 – Present

- Co-organizer and co-MC of Windows in Higher Education Conference (2003-present) - Work with Microsoft to sponsor and host five 2-3 day conferences for ~100 attendees on the Microsoft campus
- Co-admin Windows in Higher Education e-mail list (8/00-present) - Work with colleagues at other institutions to create a new technical community for higher education and grow it to more than 1500 subscribers from hundreds of institutions across the world

Conference presentations

- Educause Security Professionals Conference: Whole disk encryption and IT risk assessment
- Windows in Higher Education: Higher education collaboration on IT security
- Common Solutions Group: E-mail spam management
- Special Interest Group in University and College Computing Services (SIGUCCS): Active Directory deployment
- Multiple on-campus presentations on PCI-DSS, encryption, firewalls, IT security basics, e-mail security, Active Directory and other technologies

TECHNOLOGY EXPERIENCE

Extensive experience on the Microsoft Windows platform, ranging from security assessment to Active Directory administration to desktop support. Experience with a range of information security tools for assessment, analysis, forensics and penetration testing. **Specific technologies include:**

- Nessus vulnerability scanner
- TippingPoint Intrusion Prevention System
- PGP encryption product suite
- Q1 Qradar Security Event Manager
- Symantec Endpoint Protection, Computer Associates antivirus
- Wireshark, TCPDump, NMap
- WebScarab
- Microsoft Windows platform (NT4 - Win7)
- Microsoft Active Directory and Exchange
- Apple OS X
- Linux (Ubuntu, CentOS)
- Microsoft Office suite
- Sysinternals tool suite
- IdentityFinder, Cornell Spider, UT SENS, VT FindSSN